Craig Spencer Unit 8 Homework

Phase 1: *"I'd like to Teach the World to Ping"*

You have been provided a list of network assets belonging to RockStar Corp. Use fping to ping the network assets for only the Hollywood office.

- Determine the IPs for the Hollywood office and run fping against the IP ranges in order to determine which IP is accepting connections.

- RockStar Corp doesn't want any of their servers, even if they are up, indicating that they are accepting connections.

    - Use fping <IP Address> and ignore any results that say "Request timed out".
    - If any of the IP addresses send back a Reply, enter Ctrl+C to stop sending requests.
- Create a summary file in a word document that lists out the fping command used, as well as a summary of the results.

- Your summary should determine which IPs are accepting connections and which are not.

- Also indicate at which OSI layer your findings are found.

The below table show the IP address range for the given CDIR address

CDIR	Server Name	Start IP	End IP
15.199.95.91/28	Hollywood Database Servers	15.199.95.80	15.199.95.95
15.199.94.91/28	Hollywood Web Servers	15.199.94.80	15.199.94.95
11.199.158.91/28	Hollywood Web Servers	11.199.158.80	11.199.158.95
167.172.144.11/32	Hollywood Application Servers	167.172.144.11	167.172.144.11
11.199.141.91/28	Hollywood Application Servers	11.199.141.80	11.199.141.95

Perform an fping for the range (I could have used the CDIR address but chose to use the range option for demonstration)

```
fping -s -g 15.199.95.80 15.199.95.95
15.199.95.80 is unreachable
15.199.95.81 is unreachable
15.199.95.82 is unreachable
15.199.95.83 is unreachable
15.199.95.84 is unreachable
15.199.95.85 is unreachable
15.199.95.86 is unreachable
15.199.95.87 is unreachable
15.199.95.88 is unreachable
15.199.95.89 is unreachable
15.199.95.90 is unreachable
15.199.95.91 is unreachable
15.199.95.92 is unreachable
15.199.95.93 is unreachable
15.199.95.94 is unreachable
15.199.95.95 is unreachable

      16 targets
       0 alive
      16 unreachable
       0 unknown addresses

      16 timeouts (waiting for response)
      64 ICMP Echos sent
       0 ICMP Echo Replies received
       0 other ICMP received

 0.00 ms (min round trip time)
 0.00 ms (avg round trip time)
 0.00 ms (max round trip time)
        4.238 sec (elapsed real time)
```

```
fping -s -g 15.199.94.80 15.199.94.95
15.199.94.80 is unreachable
15.199.94.81 is unreachable
15.199.94.82 is unreachable
15.199.94.83 is unreachable
15.199.94.84 is unreachable
15.199.94.85 is unreachable
```

```
15.199.94.86 is unreachable
15.199.94.87 is unreachable
15.199.94.88 is unreachable
15.199.94.89 is unreachable
15.199.94.90 is unreachable
15.199.94.91 is unreachable
15.199.94.92 is unreachable
15.199.94.93 is unreachable
15.199.94.94 is unreachable
15.199.94.95 is unreachable

      16 targets
       0 alive
      16 unreachable
       0 unknown addresses

      16 timeouts (waiting for response)
      64 ICMP Echos sent
       0 ICMP Echo Replies received
       0 other ICMP received

 0.00 ms (min round trip time)
 0.00 ms (avg round trip time)
 0.00 ms (max round trip time)
        4.438 sec (elapsed real time)
```

fping -s -g 11.199.158.80 11.199.158.95

```
11.199.158.80 is unreachable
11.199.158.81 is unreachable
11.199.158.82 is unreachable
11.199.158.83 is unreachable
11.199.158.84 is unreachable
11.199.158.85 is unreachable
11.199.158.86 is unreachable
11.199.158.87 is unreachable
11.199.158.88 is unreachable
11.199.158.89 is unreachable
11.199.158.90 is unreachable
11.199.158.91 is unreachable
11.199.158.92 is unreachable
11.199.158.93 is unreachable
11.199.158.94 is unreachable
11.199.158.95 is unreachable
```

```
   16 targets
    0 alive
   16 unreachable
    0 unknown addresses

   16 timeouts (waiting for response)
   64 ICMP Echos sent
    0 ICMP Echo Replies received
    0 other ICMP received

 0.00 ms (min round trip time)
 0.00 ms (avg round trip time)
 0.00 ms (max round trip time)
     4.359 sec (elapsed real time)
```

```
fping -s -g 167.172.144.11 167.172.144.11
167.172.144.11 is alive

    1 targets
    1 alive
    0 unreachable
    0 unknown addresses

    0 timeouts (waiting for response)
    2 ICMP Echos sent
    1 ICMP Echo Replies received
    0 other ICMP received

 1033 ms (min round trip time)
 1033 ms (avg round trip time)
 1033 ms (max round trip time)
     1.034 sec (elapsed real time)
```

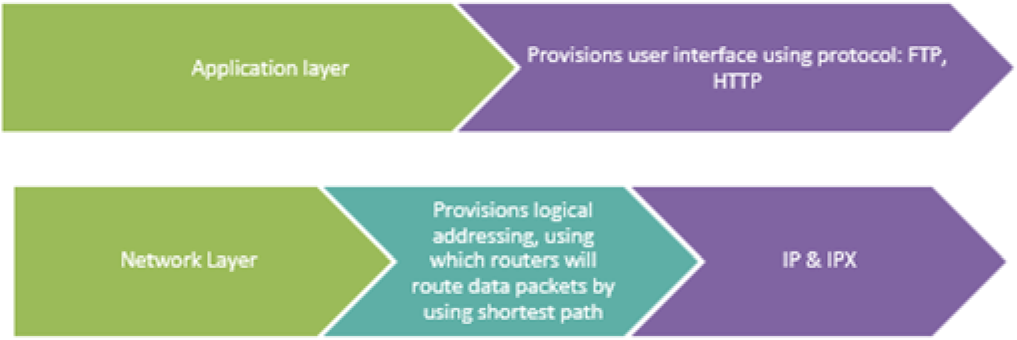
167.172.144.11 is a vulnerability as RockStar.com does not want their servers identified. This server does respond to icmp packets

```
fping -s -g 11.199.141.80 11.199.141.95
11.199.141.80 is unreachable
11.199.141.81 is unreachable
11.199.141.82 is unreachable
11.199.141.83 is unreachable
11.199.141.84 is unreachable
```

```
11.199.141.85 is unreachable
11.199.141.86 is unreachable
11.199.141.87 is unreachable
11.199.141.88 is unreachable
11.199.141.89 is unreachable
11.199.141.90 is unreachable
11.199.141.91 is unreachable
11.199.141.92 is unreachable
11.199.141.93 is unreachable
11.199.141.94 is unreachable
11.199.141.95 is unreachable

      16 targets
       0 alive
      16 unreachable
       0 unknown addresses

      16 timeouts (waiting for response)
      64 ICMP Echos sent
       0 ICMP Echo Replies received
       0 other ICMP received

 0.00 ms (min round trip time)
 0.00 ms (avg round trip time)
 0.00 ms (max round trip time)
        4.555 sec (elapsed real time)
```

Server 167.172.144.11 should have ICMP (port 21) blocked to ping requests. This leaves the servers discoverable to hackers.

Ping and fping use OSI layer 3 Network Layer as it simply a host lookup as well as the application layer.


Application layer
Provisions user interface using protocol: FTP, HTTP
Network Layer
Provisions logical addressing, using which routers will route data packets by using shortest path
IP & IPX

Phase 2: *"Some Syn for Nothin`"*

With the IP(s) found from Phase 1, determine which ports are open:

- You will run a SYN SCAN against the IP accepting connections. See **SYN SCAN Instructions** below.

- Using the results of the SYN SCAN, determine which ports are accepting connections.

- Add these findings to the summary and be sure to indicate at which OSI layer your findings were found.

```
Nmap -sS 167.172.144.11
```

```
Nmap scan report for 167.172.144.11

Host is up (0.0012s latency).

Not shown: 801 filtered ports, 198 closed ports

PORT   STATE SERVICE

22/tcp open  ssh


Nmap done: 1 IP address (1 host up) scanned in 6274.81 seconds
```

SSH tcp port 22 is open

- Findings associated with a hacker.

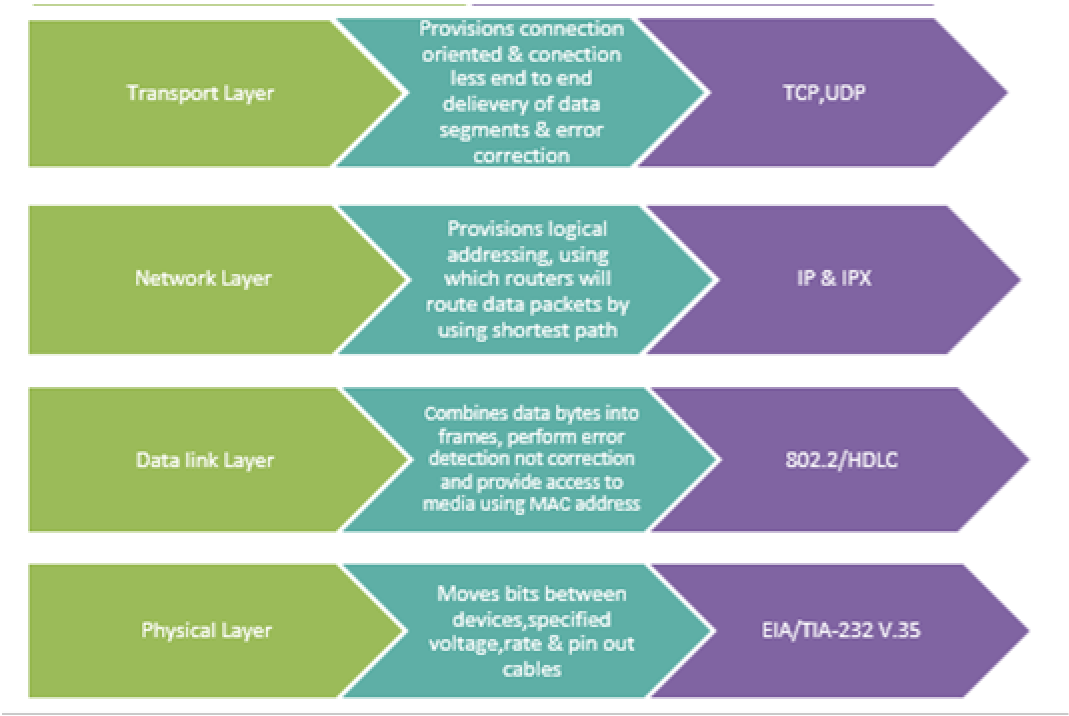
The user name Jimi and password hendrix being available suggest this has been stolen.

- Recommended mitigation strategy.

  SSH may need to be open for remote users but Jimi should change password if a genuine user at all. The company's password policy should be reviewed and increased complex, lockout rules, and password expiry should be applied. A default password for several services/applications should not be used.

- Document the OSI layer where the findings were found.

NMAp uses these OSI layers. Network layer for traceroute, transport layer for TCP and UDP and ports, and data link for protocols such as ARP.



Transport Layer	Provisions connection oriented & conection less end to end delievery of data segments & error correction	TCP,UDP
Network Layer	Provisions logical addressing, using which routers will route data packets by using shortest path	IP & IPX
Data link Layer	Combines data bytes into frames, perform error detection not correction and provide access to media using MAC address	802.2/HDLC
Physical Layer	Moves bits between devices,specified voltage,rate & pin out cables	EIA/TIA-232 V.35

If nmap -sV <address> was used then the application layer would also be used to identify version of HTTP, FTP, SSH, RDP, and SMB.

SYN SCANS run on the Transport layer.

Phase 3: *"I Feel a DNS Change Comin' On"*

With your findings from Phase 2, determine if you can access the server that is accepting connections.

- RockStar typically uses the same default username and password for most of their servers, so try this first:
  - **Username:** jimi
  - **Password:** hendrix

- Try to figure out which port/service would be used for remote system administration, and then using these credentials, attempt to log into the IP that responded to pings from **Phase 1**.
- The steps and commands used to complete the tasks.

  SSH jimi@167.172.144.11

  Use jimi credentials

  Port 22 SSH is open.

  cat /etc/hosts

- A summary of your findings for each testing phase.

```
 ssh jimi@167.172.144.11

jimi@167.172.144.11's password:

Linux GTscavengerHunt 4.9.0-11-amd64 #1 SMP Debian 4.9.189-3+deb9u1
(2019-09-20) x86_64


The programs included with the Debian GNU/Linux system are free software;

the exact distribution terms for each program are described in the

individual files in /usr/share/doc/*/copyright.


Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent

permitted by applicable law.

Last login: Thu Oct 21 13:19:33 2021 from 149.167.138.117

Could not chdir to home directory /home/jimi: No such file or directory

$ whoami

jimi

$
```

Logon was successful

- Any network vulnerabilities discovered.

The fact that the password was available suggests that it has been stolen.

Jimi has no home directory which is suspicious

```
$ cd /home

$ ls

debian matt.ryan
```

What groups is jimi subscribed to:

```
$ id

uid=1010(jimi) gid=1010(jimi) groups=1010(jimi)
```

Jimi is not a sudoer which is good.

```
$
```

Jimi can read the /etc/ passwd file to get user names

What can Jimi access?:

Ls -Ral / grep jimi list files and permissions recursively and grep for jimi to find jimi's file owner or group permissions.

```
-rwxrwxrwx  1 jimi     jimi          2 Apr 25 03:10 Brian.Hill.swp

-rwxrwxrwx  1 jimi     jimi      12288 May 10 06:09 cloud.cfg.swn

-rwxrwxrwx  1 jimi     jimi      12288 May  1 02:32 cloud.cfg.swo

-rwxrwxrwx  1 jimi     jimi      12288 May  1 02:25 cloud.cfg.swp

-rw-------  1 jimi     jimi      12288 Jul 19 09:30 config.swp

-rwxrwxrwx  1 jimi     jimi      12288 Nov 16  2020 conf.swp

-rw-------  1 jimi     jimi      12288 Aug 12 18:46 deluser.conf.swp
```

```
-rwxrwxrwx  1 jimi       jimi          266 Apr 25 07:18 dummy
-rwxrwxrwx  1 jimi       jimi        95879 Sep 24  2020 enum2.md
-rwxrwxrwx  1 jimi       jimi        48064 Apr 25 05:13 fping
-rwxrwxrwx  1 jimi       jimi       817704 Apr 27 22:20 gcc
-rwxrwxrwx  1 jimi       jimi         7381 Apr 27 21:11 grep_shadow
-rwxrwxrwx  1 jimi       jimi         1218 Jun 23 11:03 hack.sh
-rwxrwxrwx  1 jimi       jimi        12288 May  9 02:58 home.config.swp
-rwxrwxrwx  1 jimi       jimi        12288 May  9 03:15 host.config.swp
-rwxrwxrwx  1 jimi       jimi        12288 Feb 17  2021 host.conf.swp
-rw-------  1 jimi       jimi        12288 Sep 19 00:51 hosts.swh
-rw-------  1 jimi       jimi        12288 Jul 13 23:25 hosts.swi
-rwxrwxrwx  1 jimi       jimi        12288 Apr  1  2021 hosts.swj
-rwxrwxrwx  1 jimi       jimi        12288 Jan 26  2021 hosts.swk
-rwxrwxrwx  1 jimi       jimi        12288 Dec 10  2020 hosts.swl
-rwxrwxrwx  1 jimi       jimi        12288 Oct 11  2020 hosts.swm
-rwxrwxrwx  1 jimi       jimi        12288 May 30  2020 hosts.swn
-rwxrwxrwx  1 jimi       jimi        12288 May  6  2020 hosts.swo
-rwxrwxrwx  1 jimi       jimi        12288 Mar 25  2020 hosts.swp
-rwxrwxrwx  1 jimi       jimi        12288 Mar 24  2021 host.swp
-rwxrwxrwx  1 jimi       jimi           14 Apr 26 04:46 index.html
-rwxrwxrwx  1 jimi       jimi        15968 Sep 24  2020 libcap.so.2
drwxrwxrwx  2 jimi       jimi         4096 Feb 10  2021 LinEnum
-rwxrwxrwx  1 jimi       jimi       320037 Jan 27  2021 linpeas.sh
-rwxrwxrwx  1 jimi       jimi       294066 Sep 24  2020 Linpeas.sh
```

```
-rwxrwxrwx  1 jimi       jimi        171488 Apr 25 07:28 lsof
-rwxrwxrwx  1 jimi       jimi        341592 Apr 25 05:11 neofetch
-rwxrwxrwx  1 jimi       jimi       3078992 Apr 25 04:47 nman
-rwxrwxrwx  1 jimi       jimi         12288 Feb 21  2021 packetcaptureinfo.txt.swo
-rwxrwxrwx  1 jimi       jimi         12288 Feb 21  2021 packetcaptureinfo.txt.swp
-rw-r--r--  1 jimi       jimi          6718 Aug  9 23:22 ps.001
-rw-r--r--  1 jimi       jimi          6593 Aug  9 23:23 ps.002
-rw-------  1 jimi       jimi         12288 Aug 12 02:08 README.swp
-rw-r--r--  1 jimi       jimi          3338 Aug  9 23:02 recovered-sshd-configfile
-rwxrwxrwx  1 jimi       jimi            46 Apr 25 07:15 resolv.conf
-rw-------  1 jimi       jimi         12288 Aug  8 21:46 resolv.conf.swo
-rwxrwxrwx  1 jimi       jimi         12288 Jun 17  2020 resolv.conf.swp
-rw-r--r--  1 jimi       jimi           486 Aug  9 23:12 scenariolab.bash
-rwxrwxrwx  1 jimi       jimi            31 Apr 25 06:06 scriptone.sh
-rwxrwxrwx  1 jimi       jimi         12289 Feb 14  2021 server-status.conf.swp
-rw-------  1 jimi       jimi         12288 Aug 12 18:59 shell.sh.swp
-rwxrwxrwx  1 jimi       jimi         12288 Jan 27  2021 smb.conf.swp
-rwxrwxrwx  1 jimi       jimi           172 Apr 25 08:03 ssh
-rwxrwxrwx  1 jimi       jimi         12288 Mar 11  2021 sshd_config.swp
-rwxrwxrwx  1 jimi       jimi             0 Apr 25 06:33 sudoers
-rwxrwxrwx  1 jimi       jimi         12288 May  9 00:53 sudoers.swo
-rwxrwxrwx  1 jimi       jimi         12288 Mar 11  2021 sudoers.swp
-rwxrwxrwx  1 jimi       jimi         12288 Oct 21  2020 sudo.swo
-rw-------  1 jimi       jimi         12288 Feb 19  2021 .swn
```

```
-rw-------  1 jimi       jimi         12288 Nov 15  2020 .swo

-rw-------  1 jimi       jimi         12288 May 11  2020 .swp

-rwxrwxrwx  1 jimi       jimi         10240 Apr 25 07:17 systemd-private-b36515dc2bc640ebb29aa037427bb2f2-systemd-resolved.service-KImUfz.tar

-rwxrwxrwx  1 jimi       jimi       1052264 Apr 25 07:33 tcpdump

-rwxrwxrwx  1 jimi       jimi             0 Jun 23 10:49 test

-rwxrwxrwx  1 jimi       jimi          3948 Sep 24  2020 test1.sh

-rw-r--r--  1 jimi       jimi             4 Aug  9 22:54 touch-jimi

-rwxrwxrwx  1 jimi       jimi           101 Apr 25 07:54 update

-rwxrwxrwx  1 jimi       jimi         12288 Apr 23 22:45 uptime.swp

-rwxrwxrwx  1 jimi       jimi            16 Apr 25 06:42 whoami

-rwxrwxrwx  1 jimi       jimi         18992 Jun 23 11:12 ypdomainname2

drwxrwxrwx 2 jimi jimi  4096 Feb 10  2021 .

-rw-r--r-- 1 jimi jimi   658 Sep 24  2020 CONTRIBUTORS.md

-rw-r--r-- 1 jimi jimi 63915 Sep 24  2020 enum.txt

-rw-r--r-- 1 jimi jimi  1067 Sep 24  2020 LICENSE

-rw-r--r-- 1 jimi jimi 46631 Sep 24  2020 LinEnum.sh
```

Enum.txt

```
-e [-] Files owned by our user:

-rw------- 1 jimi jimi 12288 May  6 04:35 /var/tmp/hosts.swo

-rw------- 1 jimi jimi 12288 May 11 20:33 /var/tmp/.swp

-rw------- 1 jimi jimi 12288 May 30 22:31 /var/tmp/hosts.swn

-rw------- 1 jimi jimi 12288 Mar 25 20:08 /var/tmp/hosts.swp

-rw------- 1 jimi jimi 12288 Jun 17 01:16 /var/tmp/resolv.conf.swp
```

```
-rw-r--r-- 1 jimi jimi 1067 Sep 24 04:36 /var/tmp/LinEnum/LICENSE
-rw-r--r-- 1 jimi jimi 3829 Sep 24 04:36 /var/tmp/LinEnum/README.md
-rw-r--r-- 1 jimi jimi 46631 Sep 24 04:36 /var/tmp/LinEnum/LinEnum.sh
-rw-r--r-- 1 jimi jimi 658 Sep 24 04:36 /var/tmp/LinEnum/CONTRIBUTORS.md
-rw-r--r-- 1 jimi jimi 7367 Sep 24 04:50 /var/tmp/LinEnum/enum.txt
-e
```

And many more exploits and copies of shadow and other files. There are executable scripts.

These include html.index page (the startup web page when accessing the site),cloud config, host, resolv, sudoers, enumeration tools, SSH config files, and other system config tools.

Access available to the /etc/hosts file is a vulnerability.

- Findings associated with a hacker.

  Jimi has several tools and scripts which jimi has write and execute privileges.

  Jimi is not likely to be a genuine user, now seeing all these hack tools and results.

- Recommended mitigation strategy.

  Remove /var/tmp directory

  Remove jimi account and create new accounts not a generic one for all applications.

  Revoke the SSH key for jimi and renew keys for all users.

  Establish a password policy which is in line with best practice.

  Determine if SSH is required. If not, disable and remove the service. If keeping SSH ensure the SSH key password is complex.

Document the OSI layer where the findings were found.

SSH is on the application layer.

RockStar Corp recently reported that they are unable to access rollingstone.com in the Hollywood office. Sometimes when they try to access the website, a different, unusual website comes up.

- While logged into the RockStar server from the previous step, determine if something was modified on this system that might affect viewing rollingstone.com within the browser. When you successfully find the configuration file, record the entry that is set to rollingstone.com.
- PING rollingstone.com (98.137.246.8) 56(84) bytes of data.

- Terminate your ssh session to the rollingstone server, and use nslookup to determine the real domain of the IP address you found from the previous step.
    - **Note**: **nslookup** is a command line utility that can work in Windows or Linux Systems. It is designed to query Domain Name System records. You can use PowerShell or MacOS/Linux terminal to run nslookup.

    - To run **nslookup**, simply enter the following on the command line:

      nslookup <IP Address> to find the domain associated to an IP address

      OR

      nslookup <domain name> to find the IP address associated to a domain

    - You'll know you found the right domain if it begins with unknown..

Real address of rollingstone.com

```
sysadmin@UbuntuDesktop:~$ nslookup rollingstone.com

Server:         8.8.8.8

Address:        8.8.8.8#53


Non-authoritative answer:

Name: rollinstone.com

Address: 103.224.182.245
```

Bad server address - inside 167.172.144.11

```
sysadmin@UbuntuDesktop:~$ nslookup 98.137.246.8

8.246.137.98.in-addr.arpa      name = unknown.yahoo.com.


Authoritative answers can be found from:
```

The vulnerability is that the hosts file has been modified to spoof rollingstone.com to the attackers server 98.137.246.8

- $ cd /etc
- $ more hosts
- # Your system has configured 'manage_etc_hosts' as True.
- # As a result, if you wish for changes to this file to persist
- # then you will need to either
- # a.) make changes to the master file in /etc/cloud/templates/hosts.tmpl
- # b.) change or remove the value of 'manage_etc_hosts' in
- #   /etc/cloud/cloud.cfg or cloud-config from user-data
- #
- 127.0.1.1 GTscavengerHunt.localdomain GTscavengerHunt
- 127.0.0.1 localhost
- 98.137.246.8 rollingstone.com
-
- oooooooollowing lines are desirable for IPv6 capable hosts
- ::1 ip6-localhost ip6-loopback
- fe00::0 ip6-localnet
- ff00::0 ip6-mcastprefix
- ff02::1 ip6-allnodes
- ff02::2 ip6-allrouters
- ff02::3 ip6-allhosts
-

The hacker has used scripts and tools to edit the host file.

Remediate by:

Remove jimi and the /var/tmp directory

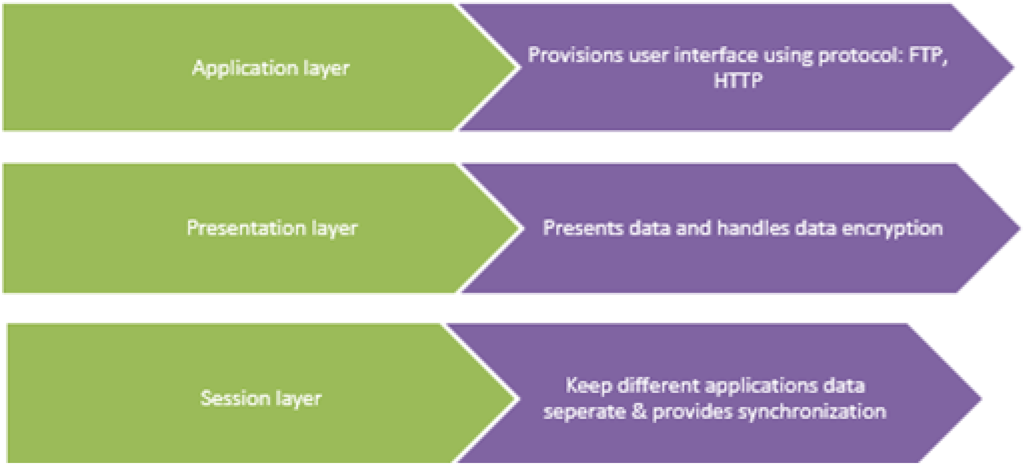
Increase security with robust password policies and lockup rules.

Audit the system to see if jimi has created other accounts, backdoors.

- Add your findings to your summary and be sure to indicate which OSI layer they were found on.

  Nslookup is an application layer application which touches the presentation and session layers.

  DNS runs on the Application layer



Application layer	Provisions user interface using protocol: FTP, HTTP
Presentation layer	Presents data and handles data encryption
Session layer	Keep different applications data seperate & provides synchronization

Phase 4: *"ShARP Dressed Man"*

Within the RockStar server that you SSH'd into, and in the same directory as the configuration file from **Phase 3**, the hacker left a note as to where he stored away some packet captures.

- View the file to find where to recover the packet captures.

cd /etc

cat packetcaptureinfo.txt

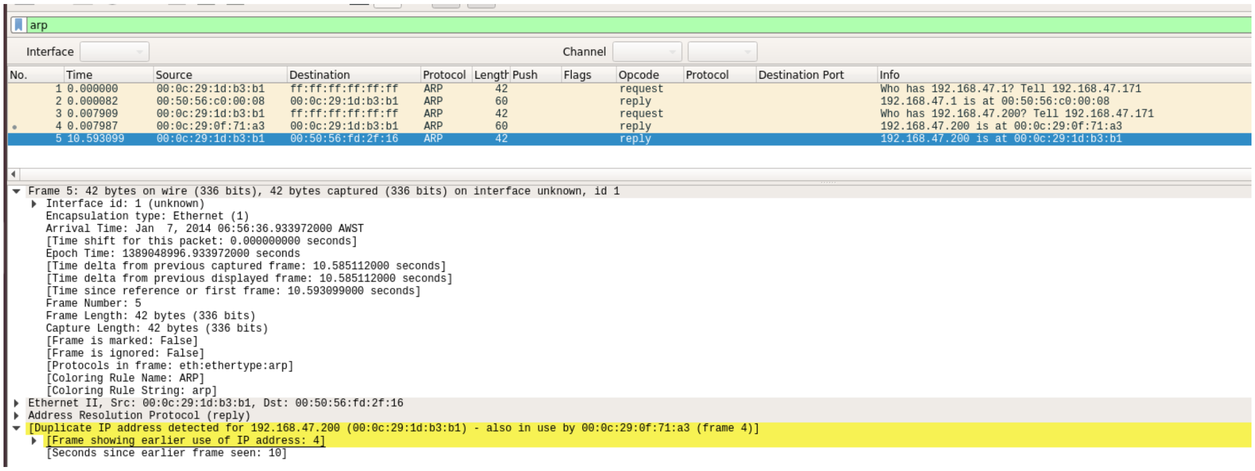
From the results of cat, extract and run

https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharintg

Download and open with wireshark

ARP.

ARP poisoning attack is occuring. Duplicate IP address detected.



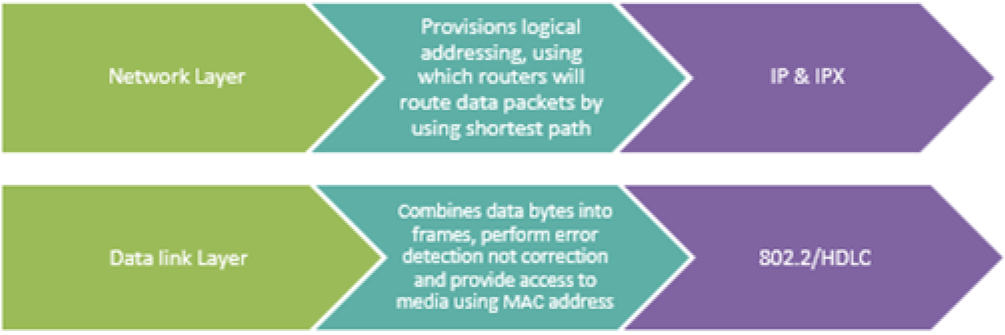
```
arp

Interface                                                    Channel

No.   Time        Source              Destination         Protocol Length Push Flags Opcode   Protocol Destination Port Info
    1 0.000000    00:0c:29:1d:b3:b1   ff:ff:ff:ff:ff:ff   ARP         42             request                            Who has 192.168.47.1? Tell 192.168.47.171
    2 0.000082    00:50:56:c0:00:08   00:0c:29:1d:b3:b1   ARP         60             reply                              192.168.47.1 is at 00:50:56:c0:00:08
    3 0.007909    00:0c:29:1d:b3:b1   ff:ff:ff:ff:ff:ff   ARP         42             request                            Who has 192.168.47.200? Tell 192.168.47.171
•   4 0.007987    00:0c:29:0f:71:a3   00:0c:29:1d:b3:b1   ARP         60             reply                              192.168.47.200 is at 00:0c:29:0f:71:a3
    5 10.593099   00:0c:29:1d:b3:b1   00:50:56:fd:2f:16   ARP         42             reply                              192.168.47.200 is at 00:0c:29:1d:b3:b1
```

```
▼ Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface unknown, id 1
  ▶ Interface id: 1 (unknown)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan  7, 2014 06:56:36.933972000 AWST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1389048996.933972000 seconds
    [Time delta from previous captured frame: 10.585112000 seconds]
    [Time delta from previous displayed frame: 10.585112000 seconds]
    [Time since reference or first frame: 10.593099000 seconds]
    Frame Number: 5
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
▶ Ethernet II, Src: 00:0c:29:1d:b3:b1, Dst: 00:50:56:fd:2f:16
▶ Address Resolution Protocol (reply)
▼ [Duplicate IP address detected for 192.168.47.200 (00:0c:29:1d:b3:b1) - also in use by 00:0c:29:0f:71:a3 (frame 4)]
  ▶ [Frame showing earlier use of IP address: 4]
    [Seconds since earlier frame seen: 10]
```

The attacker is attempting to corrupt the IP to MAC address resolution by sending replies from random MAC addresses. Not random MAC addresses. One of the MAC addresses belogs to the hacker.

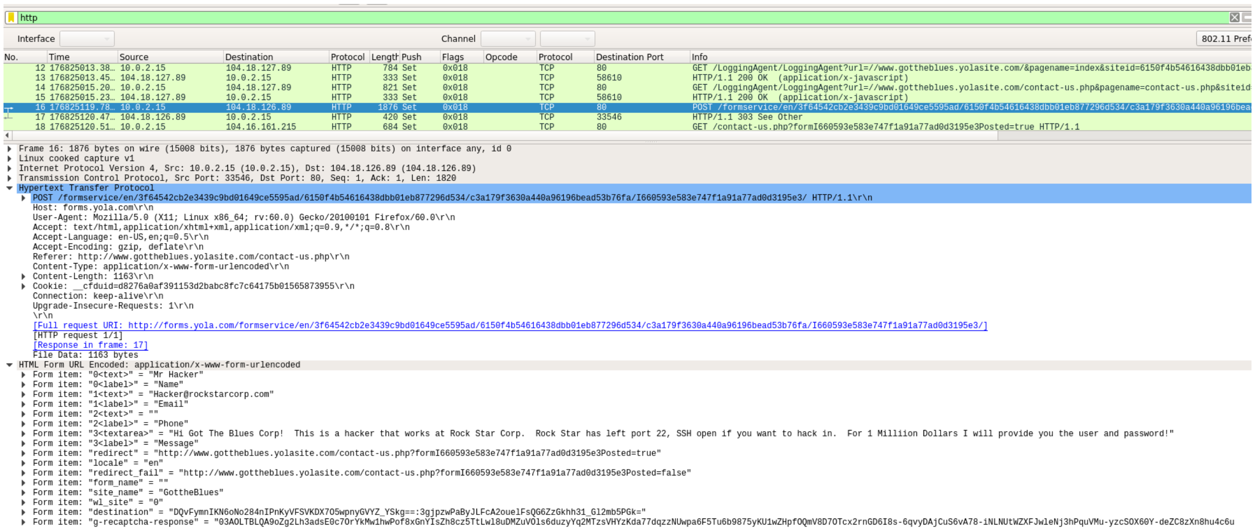
Remedy this by using static ARP entry in the server or use tools to identify ARP attacks.

ARP is used to map ip addresses to hardware address (MAC address) and operates in the network and datalink layer.


Network Layer
Provisions logical addressing, using which routers will route data packets by using shortest path
IP & IPX
Data link Layer
Combines data bytes into frames, perform error detection not correction and provide access to media using MAC address
802.2/HDLC

HTTP

Post from 10.0.2.15 has the content shown below and is attempting to redirect to: Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true"



```
No.  Time             Source         Destination     Protocol Length Push Flags Opcode Protocol Destination Port Info
  12 176825013.38…  10.0.2.15      104.18.127.89   HTTP      784 Set  0x018        TCP      80               GET /LoggingAgent/LoggingAgent?url=//www.gottheblues.yolasite.com/&pagename=index&siteid=6150f4b54616438dbb01eb
  13 176825013.45…  104.18.127.89  10.0.2.15       HTTP      333 Set  0x018        TCP      58610            HTTP/1.1 200 OK  (application/x-javascript)
  14 176825015.20…  10.0.2.15      104.18.127.89   HTTP      821 Set  0x018        TCP      80               GET /LoggingAgent/LoggingAgent?url=//www.gottheblues.yolasite.com/contact-us.php&pagename=contact-us.php&siteid
  15 176825015.23…  104.18.127.89  10.0.2.15       HTTP      333 Set  0x018        TCP      58610            HTTP/1.1 200 OK  (application/x-javascript)
  16 176825119.78…  10.0.2.15      104.18.126.89   HTTP     1876 Set  0x018        TCP      80               POST /formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb01eb877296d534/c3a179f3630a440a96196bea
  17 176825120.47…  104.18.126.89  10.0.2.15       HTTP      420 Set  0x018        TCP      33546            HTTP/1.1 303 See Other
  18 176825120.51…  10.0.2.15      104.16.161.215  HTTP      684 Set  0x018        TCP      80               GET /contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true HTTP/1.1

▸ Frame 16: 1876 bytes on wire (15008 bits), 1876 bytes captured (15008 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 104.18.126.89 (104.18.126.89)
▸ Transmission Control Protocol, Src Port: 33546, Dst Port: 80, Seq: 1, Ack: 1, Len: 1820
▾ Hypertext Transfer Protocol
  ▸ POST /formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb01eb877296d534/c3a179f3630a440a96196bead53b76fa/I660593e583e747f1a91a77ad0d3195e3/ HTTP/1.1\r\n
    Host: forms.yola.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://www.gottheblues.yolasite.com/contact-us.php\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  ▸ Content-Length: 1163\r\n
  ▸ Cookie: __cfduid=d8276a0af391153d2babc8fc7c64175b01565873955\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://forms.yola.com/formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb01eb877296d534/c3a179f3630a440a96196bead53b76fa/I660593e583e747f1a91a77ad0d3195e3/]
    [HTTP request 1/1]
    [Response in frame: 17]
    File Data: 1163 bytes
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "0<text>" = "Mr Hacker"
  ▸ Form item: "0<label>" = "Name"
  ▸ Form item: "1<text>" = "Hacker@rockstarcorp.com"
  ▸ Form item: "1<label>" = "Email"
  ▸ Form item: "2<text>" = ""
  ▸ Form item: "2<label>" = "Phone"
  ▸ Form item: "3<textarea>" = "Hi Got The Blues Corp!  This is a hacker that works at Rock Star Corp.  Rock Star has left port 22, SSH open if you want to hack in.  For 1 Milliion Dollars I will provide you the user and password!"
  ▸ Form item: "3<label>" = "Message"
  ▸ Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true"
  ▸ Form item: "locale" = "en"
  ▸ Form item: "redirect_fail" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=false"
  ▸ Form item: "form_name" = ""
  ▸ Form item: "site_name" = "GottheBlues"
  ▸ Form item: "wl_site" = "0"
  ▸ Form item: "destination" = "DQvFymnIKN6oNo284nIPnKyVFSVKDX7O5wpnyGVYZ_YSkg==:3gjpzwPaByJLFcA2ouelFsQG6ZzGkhh31_Gl2mb5PGk="
  ▸ Form item: "g-recaptcha-response" = "03AOLTBLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOls6duzyYq2MTzsVHYzKda77dqzzNUwpa6F5Tu6b9875yKU1wZHpfOQmV8D7OTcx2rnGD6I8s-6qvyDAjCuS6vA78-iNLNUtWZXFJwleNj3hPquVMu-yzcSOX60Y-deZC8zXn8hu4c6u
```

HTML Form URL Encoded: application/x-www-form-urlencoded

Form item: "0<text>" = "Mr Hacker"

Key: 0<text>

Value: Mr Hacker

Form item: "0<label>" = "Name"

Key: 0<label>

Value: Name

Form item: "1<text>" = "Hacker@rockstarcorp.com"

Form item: "1<label>" = "Email"

Form item: "2<text>" = ""

Form item: "2<label>" = "Phone"

Form item: "3<textarea>" = "Hi Got The Blues Corp! This is a hacker that works at Rock Star Corp. Rock Star has left port 22, SSH open if you want to hack in. For 1 Milliion Dollars I will provide you the user and password!"

Form item: "3<label>" = "Message"

Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true"

```
    Form item: "locale" = "en"

    Form item: "redirect_fail" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=false"

    Form item: "form_name" = ""

    Form item: "site_name" = "GottheBlues"

    Form item: "wl_site" = "0"

    Form item: "destination" = "DQvFymnIKN6oNo284nIPnKyVFSVKDX7O5wpnyGVYZ_YSkg==:3gjpzwPaByJLFcA2oueIFsQG6ZzGkhh31_GI2mb5PGk="

    Form item: "g-recaptcha-response" = "03AOLTBLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOIs6duzyYq2MTzsVHYzKda77dqzzNUwpa6F5Tu6b9875yKU1wZHpfOQmV8D7OTcx2rnGD6I8s-6qvyDAjCuS6vA78-iNLNUtWZXFJwleNj3hPquVMu-yzcSOX60Y-deZC8zXn8hu4c6u
```

The hacker is posting an html form on the contact us page () advertising the vulnerability at Rockstar and will provide the password for $1 million.

To prevent this the web administrator needs to prevent who can edit html pages. I would change ssh passwords or disable ssh if not required to prevent an attacker entering the system.

HTTP is in the application layer of the OSI model. It is a stateless protocol which uses request and response and exchanges messages across transport or session layers.

Application layer
Provisions user interface using protocol: FTP, HTTP